Journal of the Korea Convergence Society
Vol. 9. No. 9, pp. 15-22, 2018

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2018.9.9.015

광학문자인식을 이용한 사용자 인증 시스템

정필성[1], 조양현[2*]
[1]명지전문대학 정보통신공학과 조교수, [2]삼육대학교 컴퓨터·메카트로닉스공학부 교수

User Authentication System using OCR

Pil-Seong Jeong[1], Yang-Hyun Cho[2*]
[1]Dept. of Information Technology Communication, Myongji College
[2]Division of Computer & Mechatronics Engineering, Sahmyook University

요 약 스마트 기기가 보급화 됨에 따라서 사용자는 다양한 방법을 이용하여 인증 서비스를 이용할 수 있게 되었다. 인증 서비스로는 아이디와 비밀번호를 이용한 인증, 문자 메시지를 이용한 인증, OTP(One Time Password)와 같은 일회용 비밀번호를 이용한 인증 등이 있다. 본 논문은 광학문자인식 기술을 이용하여 지식기반 인증의 보안성 문제를 해결하고 쉽고 빠르게 사용자를 인증할 수 있는 인증 시스템을 제안한다. 제안하는 인증 시스템은 사용자가 업로드한 이미지에서 문자를 추출하고 추출된 문자 정보를 이용하여 사용자를 인증한다. 제안하는 인증 시스템은 외부로 쉽게 노출되거나 분실 위험이 있는 비밀번호나 OTP를 사용하지 않으며 정확한 사진을 사용하지 않으면 인증이 불가능하다는 장점을 가진다. 제안한 인증 시스템은 플랫폼에 구애받지 않으며 사용자 인증 및 파일 암호화, 복호화에도 활용이 가능하다.

주제어 : 광학문자인식, 사용자 인증, 인증 시스템, 개인정보, 정보보호

Abstract As smart devices become popular, users can use authentication services in various methods. Authentication services include authentication using an ID and a password, authentication using a sms, and authentication using an OTP(One Time Password). This paper proposed an authentication system that solves the security problem of knowledge-based authentication using optical character recognition and can easily and quickly authenticate users. The proposed authentication system extracts a character from an uploaded image by a user and authenticates the user using the extracted character information. The proposed authentication system has the advantage of not using a password or an OTP that are easily exposed or lost, and can not be authenticated without using accurate photographs. The proposed authentication system is platform independent and can be used for user authentication, file encryption and decryption.

Key Words : Optical Character Recognition, User Authentication, Authentication System, Personal Information, Information Security

1. 서론

스마트 기기가 보급화와 더불어 정보통신 기술 기반 서비스가 지역 네트워크 환경에서 클라우드 환경으로 확대됨에 따라서 정보의 유통 범위가 넓어지고 있다. 개인 스마트 기기가 보급화와 더불어 정보통신 기술 기반 서비스가 지역 네트워크 환경에서 클라우드 환경으로 확정보 침해 사고가 증가하고 있으며, 특히 가상화 서비스 기술을 이용하는 클라우드 환경에서는 개인 정보 보호에 관한 문제가 발생할 가능성이 매우 크기 때문에 개인 인

*This research was supported Basic Science Research Program through the Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2017R1D1A1B03030759)
*Corresponding Author : Yang-Hyun Cho (yhcho@syu.ac.kr)
Received June 22, 2018 Revised July 31, 2018
Accepted September 20, 2018 Published September 31, 2018

증 기술 및 개인 정보 보호를 위한 다양한 방법이 논의되고 이를 적용하기 위한 연구가 활발하게 진행되고 있다[1-3].

인증 시스템이란 정보에 접근할 수 있는 권한을 요청하는 주체가 권한을 가지고 있는지 확인해 주는 모든 과정을 인증해주는 시스템으로서 소지기반, 지식기반, 특성기반으로 분류되는 인증요소를 이용하여 인증을 진행한다. 최근에는 해킹으로부터 정보를 보호하기 위해서 금융권이나 게임 업계에서는 아이디와 비밀번호를 이용하는 1단계 인증 이후 추가적으로 OTP(One Time Password)와 같은 일회용 비밀번호를 요청하는 2단계 인증을 진행하고 있다. 하지만 OTP 서비스를 제공받을 수 있는 OTP 생성기를 항상 보관하여야 하며, 스마트폰에 설치되어 있는 OTP 인증 프로그램의 경우 OTP를 발급받기 위한 절차가 까다롭고 배터리가 없을 경우 사용할 수 없다는 문제점이 존재한다. 2단계 인증은 1단계 인증보다 안전하지만 인증절차가 복잡하고 시간이 오래 걸리기 때문에 많은 사람들이 필수적으로 이용하고 있지는 않으며 인증 서비스를 제공하는 업체들이 필수적으로 강제하고 있지는 않다[4,5].

현재 가장 많이 사용되고 있는 인증요소로는 지식기반 인증이 있으며 아이디 또는 이메일 주소와 비밀번호를 이용하여 쉽고 간단하게 인증이 이루어지는 장점이 있기 때문에 많은 사람들이 이용하고 있는 서비스이다. 하지만 지식기반 인증에서 사용하는 비밀번호는 복잡하고 길게 관리하게 되면 본인도 외우기 어렵고 본인과 연관되어 있는 숫자(생일, 주민등록번호, 핸드폰 번호 등)나 단어(영문 이니셜, 가족 영문 이름 등)를 이용하는 경우가 많아 외부로 노출되기 쉬운 단점이 존재한다. 또한 동일한 비밀번호를 여러 사이트에서 사용하는 경우가 많아 하나의 사이트에서 비밀번호가 노출되면 큰 피해를 볼 수 있으며, 비밀번호가 노출되어도 인지하기 어렵다는 문제점이 존재한다[6-8]. 사용자가 항시 휴대할 수 있는 스마트 기기를 이용하여 쉽고 간단하게 인증을 진행할 수 있는 연구로서 QR코드를 이용한 인증 방식이 존재한다. 사용자가 로그인하고자 하는 사이트에서 아이디 또는 핀 코드를 입력하면 화면에 인증을 위한 정보가 들어 있는 QR코드를 보여준다. 사용자를 자신이 가지고 있는 스마트 기기의 애플리케이션을 이용하여 카메라를 통해 QR코드를 촬영하면 해당 서버에서 인증을 진행하는 방식으로 인증절차가 진행된다. WeChat, Line, WhatsApp 서비스에서 활용되고 있으며 계정명이나 패스워드를 이용하지 않아도 쉽게 로그인할 수 있으며 랜덤한 시크릿 코드를 생성한다는 점에서 안전한 것으로 평가받았다. 하지만 최근 QR 코드 기반의 로그인 시스템 하이재킹이라 불리는 QRLJacking을 이용하여 사용자 인증을 해킹할 수 있는 기술에 위협을 받고 있다[9].

본 논문에서는 지식기반 인증처럼 쉽고 간단하면서 비밀번호를 입력하지 않기 때문에 비밀번호 유출이 불가능한 인증 시스템으로서 이미지를 이용하여 읽어낸 문자를 이용하여 사용자 인증을 진행하는 시스템을 제안한다. 제안하는 시스템은 이미지로부터 읽어낸 문자 정보를 이용하여 인증을 진행하며 약간의 이미지 변형으로도 인증이 불가능한 특성을 가지기 때문에 보안성이 높으며 어렵고 복잡한 비밀번호를 외울 필요가 없는 장점을 가진다.

본 논문의 구성은 다음과 같다. 2장에서는 구글 쿨라우드 비전 API 서비스와 인증요소 기술에 관하여 알아본다. 3장에서는 사용자 등록 및 인증을 위한 알고리즘을 알아보며 4장에서는 사용자 인증을 처리하는 시스템 구현에 대해서 알아본다. 5장에서는 효용성에 대해서 평가를 진행하며 마지막으로 6장에서는 결론을 맺는다.

2. 관련 연구

2.1 구글 클라우드 비전 API

구글 클라우드 비전 API는 구글에서 제공하는 이미지 분석 서비스로서 클라우드 기반으로 동작하며 머신 러닝 학습 모델을 이용하여 이미지 안의 개별 객체를 인식하여 수천 가지 카테고리로 분류하거나 성인 콘텐츠에서부터 폭력적인 콘텐츠에 이르기까지 다양한 유형의 부적절한 콘텐츠를 감시하는 기능을 제공한다. REST API를 제공하기 때문에 사용자가 이미지 파일에 대한 정보를 로컬 또는 리모트 상에서 제공할 수 있으며 이에 대한 메타 파일을 JSON 구조로 받을 수 있어 정보에 대한 추출 및 가공이 쉽다는 특징을 가지고 있다[10]. 본 논문에서는 OCR을 이용하여 이미지에서 텍스트 정보를 읽어내고 이 정보를 이용하여 사용자 인증에 활용한다. Table 1은 구글 클라우드 비전 API에서 제공하는 서비스 정보를 나타낸다.

Table 1. Google Cloud Vision API Feature

Feature	Description
Label Detection	Detect broad sets of categories within an image, ranging from modes of transportation to animals
Explicit Content Detection	Detect explicit content like adult content or violent content within an image
Logo Detection	Detect popular product logos within an image
Landmark Detection	Detect popular natural and man-made structures within an image
Optical Character Recognition	Detect and extract text within an image, with support for a broad range of languages, along with support for automatic language identification
Face Detection	Detect multiple faces within an image, along with the associated key facial attributes like emotional state or wearing headwear
Image Attributes	Detect general attributes of the image, such as dominant colors and appropriate crop hints
Web Detection	Search the Internet for similar images

2.2 지식기반 인증

지식기반 인증은 가장 널리 사용되는 인증방식으로서 사용자가 알고 있는 비밀번호, PIN 번호를 이용하여 인증을 진행한다[11]. 사용의 편리성 때문에 온라인 서비스에서 널리 사용되지만 비밀번호가 유출될 수 있으며 동일한 비밀번호를 여러 서비스에 사용하는 경우가 많아 비밀번호가 유출되면 여러 서비스에서 개인 정보가 노출될 수 있다는 문제점이 존재한다.

2.3 소지기반 인증

소지기반 인증은 사용자가 소유한 것을 이용하는 인증방법으로 일회용비밀번호(OTP), 보안토큰(HSM), 스마트카드 등을 이용하는 방법이다. 소지기반 인증은 아이디, 비밀번호를 입력하는 1단계 인증 이후 2단계 인증으로 인증절차가 이루어지는 구글 로그인 서비스, 게임 서비스 등에서 사용된다. 인터넷 뱅킹에서는 이체시 OTP를 인증수단으로 활용하여 현재 로그인한 사용자가 본인이 맞는지 다시 확인한다[12]. 소지기반 인증서비스는 사용이 편리하지만 휴대의 문제가 발생할 수 있다.

2.4 특성기반 인증

특성기반 인증은 사용자만이 소유할 수 있는 고유한 특성 정보를 이용하여 인증을 진행하는 방식이다. 특성기반 인증요소로는 홍채, 목소리, 지문 등이 있다. 출입문 인증을 위해서 사용자의 지문을 이용하게 되면 쉽고 편리하게 인증이 이루어질 수 있다[13]. 하지만 사용자의 몸 상태에 따라서 인증정보가 변할 수 있으며 인증을 위해서 사용자의 홍채, 목소리, 지문 정보를 서버에서 보관, 관리하고 있어야 하는 이유로 개인 정보 노출에 대한 관리가 필요하다.

2.5 기타 인증요소

최근에는 정보통신 기기의 발전으로 지식기반, 소지기반, 특성기반과 같은 전통적인 인증방식 이외의 방법으로 인증을 처리하는 방법에 대한 연구가 활발하게 이루어지고 있다. GPS를 이용한 사용자의 위치정보, 블루투스, 와이파이와 같은 사용자가 소유하고 있는 스마트폰에서 획득할 수 있는 정보, 가속도 센서를 이용하여 사용자의 패턴을 분석하여 인증하는 기술 등 다양한 방법에 대한 논의가 이루어지고 있다. 하지만 환경조건 및 사용자의 상태에 따라서 변이가 심하기 때문에 실사용에서 적용하기 위해서는 많은 정보를 수집하고 이를 분석하는 빅데이터 기술과 머신러닝에 대한 연구가 수반되어야 한다[14,15].

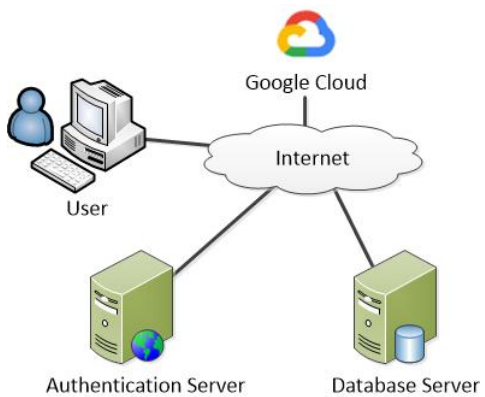

Fig. 1. Proposed Network Model

3. 제안 시스템 알고리즘

3.1 제안 네트워크 모델

제안 시스템의 네트워크 모델은 Fig. 1과 같다. 제안 시스템은 웹 서비스를 기반으로 동작한다. 사용자의 웹

브라우저를 이용하여 서비스를 제공하기 위한 인증서버는 웹 서비스 및 인증을 처리한다. 문자인식모듈을 이용하여 광학문자인식을 위한 구글 클라우드 서버와 통신하며 인식된 문자를 이용하여 인증에 이용한다. 데이터베이스 서버에는 인증 정보가 보관되어 있다.

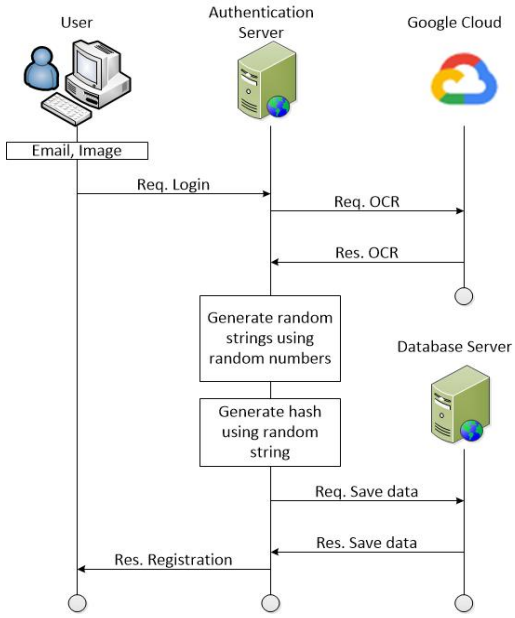

Fig. 2. User Registration Flow

3.2 사용자 등록

Fig. 2는 사용자 등록을 위한 절차를 나타낸다. 사용자는 등록 과정 중에 아이디와 문자가 포함되어 있는 이미지를 웹 서버로 전송한다. 웹 서버는 광학문자인식 모듈을 이용하여 문자 정보를 추출하여 암호화 후 아이디와 함께 데이터베이스에 저장한다. 처리되는 과정 중에 암호화에 사용되는 정보는 사용자도 알 수 없기 때문에 비밀번호를 문자입력과 같은 방식으로 처리하는 과정에서 발생하는 비밀번호 유출 및 분실의 문제점이 없으며 이미지만을 사용하기 때문에 사용자 입장에서는 인증 처리가 단순하게 이루어지는 구조를 가진다. 사용자 등록을 위한 세부 동작은 다음과 같다.

① 사용자는 인증에 사용할 이메일과 이미지를 서버로 전송한다.

② 인증서버에서 사용자 정보를 확인하여 등록되어 있는 사용자가 아닐 경우 사용자 등록 과정을 진행한다.

③ 광학문자인식 모듈을 이용하여 전송된 이미지에서 문자 정보를 추출한다.

③ 추출된 문자 정보에서 무작위적인 문자를 추출하고 이를 이용하여 새로운 문자열을 만들어낸다.

④ 새롭게 생성한 문자열을 이용하여 단방향 해시를 생성하고 이미지 정보를 파기한다.

⑤ 이메일, 비밀번호(단방향 해시), 무작위 문자 추출에 사용된 난수 정보를 데이터베이스에 저장하여 등록을 마친다.

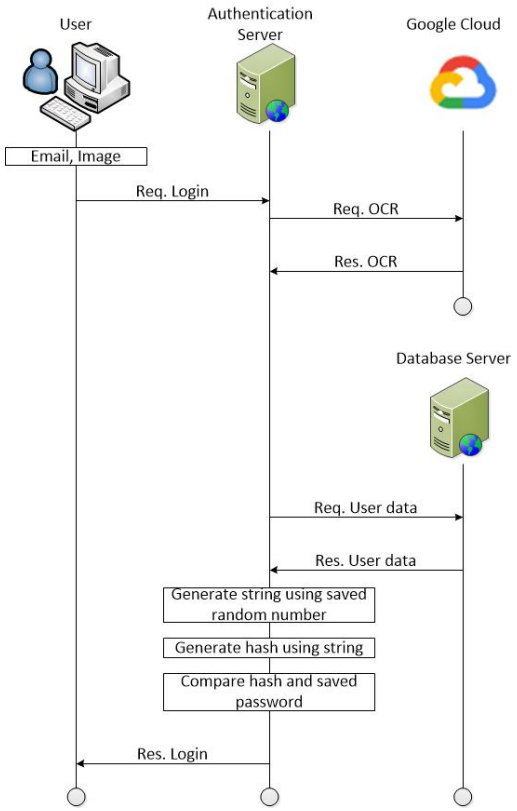

Fig. 3. User Login Flow

3.3 사용자 로그인

Fig. 3은 사용자 로그인을 위한 절차를 나타낸다. 사용자는 로그인을 위해서 아이디와 문자가 포함되어 있는 이미지를 웹 서버로 전송한다. 웹 서버는 광학문자인식 모듈을 이용하여 문자 정보를 추출하고 데이터베이스에서 문자정보를 이용하여 생성한 단방향 해시와 데이터베이스에 등록된 사용자 해시를 비교한다. 인식되는 문자가 정확하게 일치되는 이미지를 사용하지 않을 경우 로

그인이 불가능하기 때문에 옆에서 다른 사람이 훔쳐보더라도 어떤 이미지를 사용하는지 유추가 어렵다는 장점이 있다. 사용자 로그인을 위한 세부 동작은 다음과 같다.

① 사용자는 인증에 사용할 아이디와 이미지를 서버로 전송한다.

② 인증서버에서 사용자 정보를 확인하여 등록되어 있는 사용자일 경우 사용자 로그인 과정을 진행한다.

③ 광학문자인식 모듈을 이용하여 전송된 이미지에서 문자 정보를 추출한다.

④ 데이터베이스로부터 사용자 등록에 사용된 난수를 받아온다. 추출된 문자 정보에서 난수를 이용하여 새로운 문자열을 만들어낸다.

⑤ 새롭게 생성한 문자열을 이용하여 단방향 해시를 생성하고 이미지 정보를 파기한다.

⑤ 생성한 단방향 해시정보와 데이터베이스 서버로부터 받아온 해시 정보를 비교하여 사용자 인증을 진행한다.

4. 제안 시스템 구현

제안 사용자 인증 알고리즘이 적용된 시스템을 구현하기 위해서 웹 서버는 Apache 서버를 이용하였으며, 웹 프레임워크로는 파이썬 플라스크를 이용하였으며 기능 모듈은 파이썬으로 구성하였다. 데이터베이스 MariaDB를 이용하여 대용량의 데이터 처리를 지원할 수 있도록 구성하였다. Table 2는 사용자 인증을 위해서 사용되는 테이블을 나타낸다. 테이블은 USERS로 하였다. 구성된 필드는 정보 구분자로 사용되는 id, 사용자 이메일 주소를 저장하는 email, 사용자 비밀번호를 저장하는 passwd로 구분된다. passwd 필드에 저장된 정보는 해시 정보로서 외부로 노출되더라도 직접적으로 활용이 불가능하다.

Table 2. USERS Table Scheme

Field	Type	Etc
id	INTEGER	PRIMARY KEY AUTO INCREMENT NOT NULL
email	VARCHAR(100)	NOT NULL
passwd	VARCHAR(255)	NOT NULL

사용자 인증에 사용되는 단방향 해시를 생성하기 위해서 사용되는 무작위 문자 추출용 난수를 저장하기 위한 테이블을 Table 3과 같이 구성하였다. 테이블은 RANDS로 하였다. 구성된 필드는 정보 구분자로 사용되는 id, 난수를 저장하는 rand, USERS 테이블의 구분자를 외래키로 저장하는 user_id로 구분된다.

Table 3. RANDS Table Scheme

Field	Type	Etc
id	INTEGER	PRIMARY KEY AUTO INCREMENT NOT NULL
rand	VARCHAR(100)	NOT NULL
user_id	INTEGER	FOREIGN KEY(USERS.id) NOT NULL

Fig. 4는 사용자 등록 진행하는 화면이다. 사용자 등록을 위해서 사용할 이메일과 파일을 서버로 전송한다.

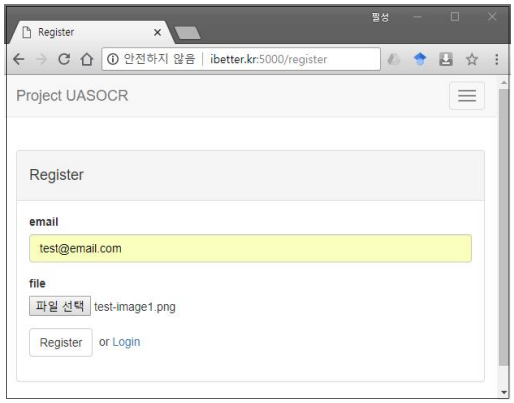

Fig. 4. User Registration Screen

Fig. 5는 인증 서버에서 사용자를 정상적으로 등록한 화면이다. 서버에서는 올바르게 사용자 등록이 처리된 경우 추출한 문자, 추출한 무작위 문자, 생성된 단방향 해시를 화면에 보여준다. 등록에 사용한 이미지는 다른 사람이 유추가 어렵도록 글씨가 잘려있는 이미지를 사용하였다. Fig. 6은 인증에 실패한 화면과 사용한 이미지를 보여준다. 인증을 위해 사용한 이미지는 글씨가 전체가 보이는 이미지로서 사용자가 인증을 위한 이미지를 유추하기 어렵다는 것을 보여준다.

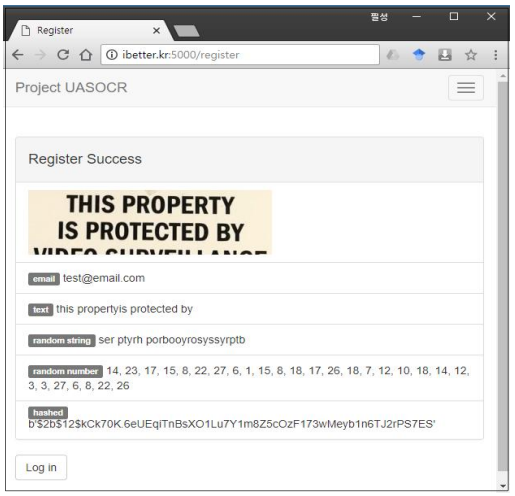

Fig. 5. User Registration Result Screen

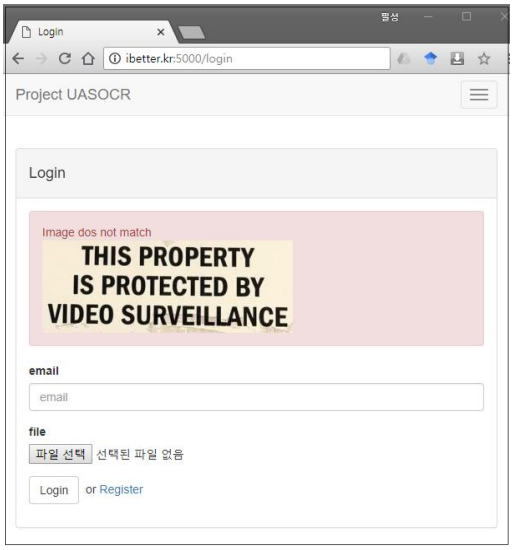

Fig. 6. User Authentication Fail Screen

5. 제안 시스템 효용성 평가

한국인터넷진흥원에서는 본인확인수단의 적합성 기준으로 보편성, 유일성을 기준으로 제시하였다. 인증서비스 제공하는데 있어서는 경제성과 법적 타당성(서비스의 명확성)이 논의되어야 하며 사용자 입장에 있어서 대체수단의 범용성 및 인증의 신뢰성이 논의되어 되어야한다. 본 논문에서는 인증기술의 기술로 적용성(적용 가능성, 적용 비용, 기술 중립성, 기존인프라 활용성), 보안성(오프라인 공격대응, 온라인 공격대응, 거래조작 공격대응), 편의성(소지사용, 발급, 교육 편의성)을 기준으로 효용성에 대해서 평가한다.

5.1 적용성

적용성이란 다양한 환경과 다양한 기기에 적용이 가능한지 여부를 말한다. 카메라가 내장되어 있거나 카메라를 연동할 수 있는 스마트 기기 또는 이미지 파일을 보관이 가능한 기기라면 쉽게 적용이 가능하며 광학문자인식 기술을 기기 자체적으로 적용도 가능하기 때문에 금융 서비스, 게임 서비스 등 다양한 인증 서비스에 널리 활용이 가능하다.

5.2 보안성

보안성이란 지속 발전하는 해킹에 대한 대응력을 말한다. 보관 및 취급이 쉬운 이미지 파일을 이용하지만 이미지에 있는 문자를 이용하기 때문에 타인이 훔쳐보더라도 내부의 이미지 문자를 이용하는 것이 어렵고 책과 같은 내용을 사진으로 찍어 활용하면 동일한 문자가 인식되는 상황을 예측하기 어려워 해킹에 대한 방어수단으로 적용할 수 있다.

5.3 편의성

편의성이란 이용이 간편하고 휴대가 용이하여 언제 어디서나 쉽게 인증에 적용할 수 있는 인증기술인지를 말한다. 본 논문에서 제안하는 광학문자인식을 이용한 사용자 인증 시스템은 웹 검색을 통해서 쉽게 구할 수 있는 이미지를 활용하거나 사용자의 스마트 기기를 이용하여 찍은 사진을 활용할 수 있기 때문에 소지가 간편하다. 또한 사진이 없더라도 해당 하는 이미지의 출처 또는 장소를 알고 있으면 쉽게 구할 수 있기 때문에 쉽게 인증이 이루어질 수 있는 기술로 평가할 수 있다.

6. 결론

스마트폰 이용자수가 증가하고 있으며 급증하고 있으며 Pew Research Center의 발표에 따르면 2015년 3월 기준으로 대한민국은 UAE(90.8%), 싱가포르(87.7%), 사우디 아라비아(86.1%)에 이어 83.0%의 보급률로 4위를 기록하고 있다. 그 중 금융 결제 서비스를 이용하며 경제적

영향력을 행사할 수 있는 성인인구의 82%인 33,929,961명이 스마트폰을 사용하고 있다. 정보기술의 발전으로 다양한 인증 방식이 도입되고 있지만 해킹으로부터 안전하지 못하며 계정에 대한 정보 관리는 여전히 개인적인 문제로 남겨져 있다. 본 논문에서는 서비스 제공자 및 사용자 입장에서 보안성이 확보된 상태에서 쉽고 편리하게 인증을 진행할 수 있는 인증 서비스를 제안하였다. 제안한 시스템은 항시 휴대하는 스마트폰을 이용하거나 자주 사용하는 개인용 컴퓨터에서 이메일과 이미지 파일을 이용하여 인증에 사용한다. 이미지 파일은 보관 및 취득이 쉽지만 이미지 파일에 있는 문자를 이용하여 인증을 진행하기 때문에 사용자는 안전하게 인증정보를 보호할 수 있다는 장점이 있다. 본 연구를 초석으로 하여 딥러닝 기반의 객체인식과 함께 문자 정보를 조합한 다중조합인증 알고리즘에 대한 확장 연구를 계획 중이며 향후 클라우드 기반의 문서 및 파일 관리를 위한 시스템에 적용할 예정이다.

REFERENCES

[1] Y. Ko, J. Choi & B. Kim. (2012). Protecting Individuals from Secondary Privacy Loss using Breached Personal Data Information Center, *Journal of the Korea Institute of Information Security & Cryptology*, 22(2), 391-400.

[2] T. Y. Kim, H. J. Jun & T. S. Kim. (2018). An Analysis on Intention to Use Information Service for Personal Information Breach, *Journal of the Korea Institute of Information Security & Cryptology*, 28(1), 199-213.

[3] T. H. Park, G. R. Lee & H. W. Kim. (2017). Survey and Prospective on Privacy Protection Methods on Cloud Platform Environment, *Journal of the Korea Institute of Information Security & Cryptology*, 27(5), 1149-1155.
DOI : 10.13089/JKIISC.2017.27.5.1149

[4] H. J. Mum, (2018). Biometric Information and OTP based on Authentication Mechanism using Blockchain, *Journal of Convergence for Information Technology*, 8(3), 85-90.

[5] S. H. Lee, (2014). User Authentication Using Biometrics and OTP in Mobile Device, *Journal of Convergence for Information Technology*, 4(3), 27-31.

[6] S. S. Ji, (2012). The Improved-Scheme of Two Factor Authentication using SMS, *Journal of the Korea Industrial Information Systems Research*, 17(6), 25-30.
DOI : 10.9723/jksiis.2012.17.6.025

[7] S. J. Kim & S. S. Yeo, (2013). A Study on Secure Data Access Control in Mobile Cloud Environment, *Journal of Digital Convergence*, 11(2), 317-322.

[8] H. T. Chae & S. J. Lee, (2014). Security Policy Proposals through PC Security Solution Log Analysis - Prevention Leakage of Personal Information, *Journal of the Korea Institute of Information Security & Cryptology*, 24(5), 961-968.
DOI : 10.13089/JKIISC.2014.24.5.961

[9] S. Khandelwal. (2016). QRLJacking – Hacking Technique to Hijack QR Code Based Quick Login System. The Hacker New(Online). https://thehackernews.com/2016/07/qrljacking-hacking-qr-code.html

[10] Google. (2018). Google Cloud Vision API. Google Cloud Vision(Online). https://cloud.google.com/vision

[11] Y. J. Shin, S. H. Shin, J. S. Lee & W. G. Han, (2015). A Study on Improvement of Identification Means in R.O.K, *Journal of Korean Associastion for Regional Information Society*, 18(4), 59-88.

[12] D. J. Kim & H. S. Choi, (2009). Design on Protection and Authentication System of IPTV Contents using OTP, *Journal of The Korea Ccontens Association*, 9(8), 129-137.
DOI : 10.5392/JKCA.2009.9.8.129

[13] C. J. Chae, H. J. Cho & H. M. Jung, (2018). Authentication Method using Multiple Biometric Information in FIDO Environment, *Journal of Digital Convergence*, 16(1), 159-164.

[14] J. S. Seo & J. S. Moon, (2015). A Study on User Authentication with Smartphone Accelerometer Sensor, *Journal of The Korea Institute of Information Security and Cryptology,* 25(6), 1477-1484.
DOI : 10.13089/JKIISC.2015.25.6.1477

[15] H. Ketabdar, K. A. Yuksel, A. Jahnbekarn, M. Roshandel & D. Skirop, (2010). MagiSign: User Identification /Authentication Based on 3D Around Device Magnetic Signatures, *Proc. Of UBICOMM'10*, 31-34.

정 필 성(Jeong, Pil Seong) [정회원]

- 2014년 2월 : 서울과학기술대학교 전자공학과(공학사)
- 2007년 8월 : 광운대학교 전자통신공학과(공학석사)
- 2013년 8월 : 광운대학교 전자통신공학과(공학박사)
- 2018년 3월 ~ 현재 : 명지전문대학 정보통신공학과 조교수
- 관심분야 : 사물인터넷, WSN, 임베디드 시스템
- E-Mail : ibetter.kr@gmail.com

조 양 현(Cho, Yang Hyun) [정회원]

- 1982년 2월 : 광운대학교 전자통신공학과(공학사)
- 1985년 2월 : 광운대학교 전자통신공학과(공학석사)
- 2012년 2월 : 광운대학교 전자통신공학과(공학박사)
- 1987년 9월 ~ 1997년 8월 : LG정보통신 전송기술개발실 과장
- 1997년 9월 ~ 현재 : 삼육대학교 컴퓨터●메카트로닉스공학부 교수
- 2014년 3월 ~ 2016년 2월 : 삼육대학교 산학협력단장/연구처장
- 관심분야 : 컴퓨터네트워크, 통신망(BcN), GMPLS, IoT
- E-Mail : yhcho@syu.ac.kr